Response to the Pre-Bid Queries , Technical Specifications , to the RFP Procurement of Network Gateway Security Products, Implementation & Management.
(Next Generation Firewall Solution, Sandbox Solution, DNS Security etc.) Ref: LIC-CO/IT-BPR/FW/RFP/2022-23/01 Dated: 21/10/2022

Sr. No.	RFP Document Reference(s) (Section & Page Number)	RFP Clause	Pre-bid Queries	Response
1	General Requirements (1.3)	The proposed application security solution must be in the Leader's or Challengers quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the last three published reports. This clause will not be applicable for the OEMs qualifying under Make in India category.	It is highly recommended to consider only Gartner's Leader quadrant and not challengers as core security solution is of prime importance. We request customer to amend the point and keep it specifically for vendors in Leader quadrant.	Please be guided by the RFP
2	General Requirements (1.10)	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades	1. Check Point has a different workflow here, the solution takes a snapshot (backup of configuration along with the OS) before version upgrades to have it auto-rollback in case of any issues identified while upgrading. 2. The same Snapshot can be stored externally on another storage 3. The solution has a feature named pre-upgrade verifier which verifies the problem / compatibility of the hotfixes / OS on the current platform and showcases the result to have a seamless & successful upgrade. Requesting LIC team to kindly acknowledge and accept this approach as compliant.	Please refer to the revised technical specifications
3	Performance (2.1)	Cluster based solutios will not be acceptable.	Check Point supports HyperScale solution i.e. Quantum Maestro which is a highly scalable solution. Request LIC to consider the solution OR else remove the Cluster clause.	Please be guided by the RFP
4	Performance (2.6)	The proposed appliance must have 256 GB of RAM from day one	Request relaxation to reduce it to 128GB or removal of this clause, this will enable us to quote.	Please refer to the revised technical specifications
5	Threat Prevention Features (6.3)	Shall support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness	The current landscape is highly evolved and so is the number of applications. In the current generation of available technologies the number of applications support should atleast be 9000 or more to have better visibility. Requesting LIC team to amend the same.	Please be guided by the RFP
6	Threat Prevention Features (6.12)	Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence	This point focuses more on endpoint needs. Requesting LIC team to remove it and keep it specific to Network Firewalls only.	Please refer to the revised technical specifications
7	Threat Prevention Features	Additional Suggestion	To have uniformity of requirement around the common technologies (Firewall, Application Control, Threat Prevention), we would request LIC team to have the same specifications as mentioned in "Perimeter DC" to get the best of features available for this technology. For e.g. addition of clauses 4.1 to 4.15, 5.13 to 5.21, 5.24 to 5.31, 5.38 to 5.56 etc.	Please be guided by the RFP
8	Management & Reporting (8.3)	Solution should support minimum 10TB of usable storage space for logs and reporting along with RAID-6 redundancy	We will recommend storing the logs on external device instead on the management server to increase it capabilities OR instead go ahead with a software based option as it is the recommended industry practice to tweak the hardware parameters as per LIC's requirement and is very flexible. Requesting LIC team to amend it to below: The management server can be quoted as a software management so that LIC team has the control on tweaking the specifications as and when required.	Please refer to the revised technical specifications
9	Management & Reporting (8.20)	Management solution should also have the following operational capabilities: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. Ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on Firewall Rules sets	There are dedicated tools available which has these requirements as a part of their use cases and many additional features over it. We would request LIC team to remove this point and have this covered under dedicated tools.	Clause Deleted
10	General Requirements - 1.12	The OEM must provide minimum 3 reference customer of same hardware & product model in India.	Considering that the Firewall has to be available with 6 years of support, we would be proposing the latest generation of firewall. Hence we request you to consider the clause as below. "The OEM must provide minimum 3 reference customer of same / similar / higher hardware model in India."	Please refer to the revised technical specifications
11	Performance - 2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable.	Throughput consideration in terms of packet size and protocol should be similar for both Perimeter and Core firewall as same application traffic will pass through both tiers of firewall. Considering different benchmarks for sizing Perimeter and Core firewall may lead to variance in firewall performance at both tiers. Public document contains throughput based on enterprise mix of traffic and not HTTP 64K with all the features enabled. We can provide the undertaking on for the throughput. Request to change the clause as "The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 64K. The claim has to be supported by publicly available documents published prior to the date of this RFP or OEM undertaking on Letterhead. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable."	Please refer to the revised technical specifications

12	Performance - 2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable.	The clause mentions throughput requirement of 30Gbps with ingress throughput of 30Gbps and outgress throughput of 30Gbps simultaneously. The firewall is sized based on the total throughput of the appliance. Irrespective of the direction, traffic will hit and be processed by the CPU of the firewall. Request you to confirm if the throughput should be considered at 60Gbps (aggregation of ingress + outgress traffic).	Please refer to the revised technical specifications
13	2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and shouuld not be for a cluster. Cluster based solutions will not be acceptable.	Request to mention the exact throughput value. Ingress & Egress calculation is confusing as the minimum throughput is 30GB then Ingress & Egress should be 15GB. We calculate throughput based on Incoming ingress traffic plus Incoming Egress traffic. Request to clarify this. Request to change the performace on TCP-IP	Please refer to the revised technical specifications
	2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and shouuld not be for a cluster. Cluster based solutions will not be acceptable.	Request to mention the exact throughput value. Ingress & Egress calculation is confusing as the minimum throughput is 30GB then Ingress & Egress should be 15GB. We calculate throughput based on Incoming ingress traffic plus Incoming Egress traffic. Request to clarify this. Request to change the performace on TCP-IP	Please refer to the revised technical specifications
14	High Availability - 3.13.5	The Firewall must support (redundant) Field replaceable (FRU) and hot swappable AC power supply and Hot swappable FAN. It must be supplied with both the Indian as well as European standard compatible power cords.	The proposed firewall will have in-built redundant FANs to ensure that the internal components are provided sufficient cooling and resiliency to failure. It does not give any additional benefit from a hardware standpoint. Request you to modify the clause as " The Firewall must support (redundant) Field replaceable (FRU) and hot swappable AC power supply and redundant FAN. It must be supplied with both the Indian as well as European standard compatible power cords..	Please be guided by the RFP
15	Threat Prevention - 6.4	The Proposed Solution should support over 40K IPS Signature.	It is important for the solution to have effective security instead of relying on the number of IPS signatures. Similar criteria should be considered for Core firewall as considered for Perimeter firewall. Request to rephrase the clause inline to the perimeter firewall specification as following "Security effectiveness should be certified by NSS and should be more than 98.5%. In case NSS Lab reports are not published in the last two years prior to the date of this RFP, the OEM should have AAA rating published by Cyber rating report in 2021 ."	Please refer to the revised technical specifications
16	Threat Prevention - 6.13	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	NetBIOS (Network Basic Input/output System) is a network service that enables applications on different computers to communicate with each other across a local area network (LAN). It was developed in the 1980s for use on early, IBM-developed PC networks. In order to have faster file transfers users use reliable protocols like FTP / SFTP. Similar protocol like CIFS was introduced later in Windows. Request you to rephrase the point as "Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN/CIFS and FTP"	Please be guided by the RFP
17	Management & Reporting - 8.4	The solution has to provide for taking backups encrypted in SHA-256 format.	Every vendor uses different encryption methods to encrypt the backup files. We support AES-128. Request you to rephrase the clause as "The solution has to provide for taking backups in encrypted in SHA-256 / AES/128 format."	Please refer to the revised technical specifications
18	Management & Reporting - 8.6	The solution must be able to segment the rule based sub policy structures in which only the relevant traffic is being forwarded to relevant policy.	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP
19	Management & Reporting - 8.20	Management solution should also have the following operational capabilities: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets	Features like Rule consolidation, overly permissive rule and rule reordering are supported by single OEM. Request you to remove these points from the requirement.	Clause Deleted
20	Management & Reporting - 8.28	Solution must support copy-pasting between security policies.	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP
21	Management & Reporting - 8.31	Solution must support adding exceptions to IPS enforcement from the log record	As log access is available with different levels of administrator, this feature can lead to security concerns if IPS exceptions are added which can lead to bypassing of genuine attacks. Request you to remove this clause.	Clause Deleted
22	API Automation - 9.3	The solution should support Management API for IoC Blocking	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP
23	API Automation - 9.4	The solution should support Add, delete, and view indicators through the management API	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP

24	2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and shouuld not be for a cluster. Cluster based solutions will not be acceptable.	Request to mention the exact throughput value. Ingress & Egress calculation is confusing as the minimum throughput is 30GB then Ingress & Egress should be 15GB. We calculate throughput based on Incoming ingress traffic plus Incoming Egress traffic. Request to clarify this. Request to change the performace on TCP-IP	Please refer to the revised technical specifications
25	8.3	Solution should support minimum 10 TB of usable storage space for logs and reporting along with RAID-6 redundancy.	Request to change to "Solution should support minimum 10 TB of storage space for logs and reporting along with RAID-6 redundancy."	Please refer to the revised technical specifications
26	8.22	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other	Working parallel on same policy can result in conflict of the policy and the policy deployment might not be reflecting the latest changes. Hence requesting to remove this clause	Clause Deleted
27	1.9	The proposed appliance must natively support (without breakout) 8 x 1G Copper & 8 x 10G SFP+ Ports from day one. The 1G Copper ports should also support 10 SFP+ transceivers and the 10 SFP+ ports should also support 1 G Copper ports .The appliance should have 2 x 100G QSFP ports. Management,sync,HA etc ports should be additional. All the modules and transceivers should be provided from day one. (16x1 GCopper , 16x10G SFP , 2x100G QSFP in addition to the management , sync and HA ports	Requesting you to change the clause as "The 1G Copper ports should also support 10 SFP+ transceivers and the 10 SFP+ ports should also support 1 G Copper ports (Optional or at least for 50% ports)" Since interchanging the transceivers on all ports might not needed. (8x10Gb transceivers can accommodate 4x1GB copper)	Please refer to the revised technical specifications
28		Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades	Bidder requests LIC to consider alternate methods of Snapshot based backups and autorollbacks in case of any issues identified while upgrading. This can be stored externally also in another storage . Pre-upgrade verifiication mechanism verifies the problem / compatibility of the hotfixes / OS on the current platform and showcases the result to have a seamless & successful upgrade. Requesting LIC team to kindly acknowledge and also accept this approach as compliant.	Please refer to the revised technical specifications
29	Performance (2.1)	Cluster based solutios will not be acceptable.	Bidder requests LIC to consider Hyperscale solution or delete the clause	Please be guided by the RFP
30	Performance (2.6)	The proposed appliance must have 256 GB of RAM from day one	Bidder requests relaxation to reduce it to 128GB	Please refer to the revised technical specifications
31	Threat Prevention Features (6.3)	Shall support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness	Bidder requests LIC to consider the number of applications support for atleast be 9000 or more to have better visibility	Please be guided by the RFP
32	Threat Prevention Features (6.12)	Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence	Bidder understands that this point focuses more on endpoint needs. Requesting LIC team to delete the clause and keep it specific to Network Firewalls only	Please refer to the revised technical specifications
34	2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and shouuld not be for a cluster. Cluster based solutions will not be acceptable.	Request to mention the exact throughput value. Ingress & Egress calculation is confusing as the minimum throughput is 30GB then Ingress & Egress should be 15GB. We calculate throughput based on Incoming ingress traffic plus Incoming Egress traffic. Request to clarify this. Request to change the performace on TCP-IP	Please refer to the revised technical specifications
35	8.3	Solution should support minimum 10 TB of usable storage space for logs and reporting along with RAID-6 redundancy.	Request to change to "Solution should support minimum 10 TB of storage space for logs and reporting along with RAID-6 redundancy."	Please refer to the revised technical specifications
36	8.22	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other	Working parallel on same policy can result in conflict of the policy and the policy deployment might not be reflecting the latest changes. Hence requesting to remove this clause	Clause Deleted
37	1.9	The proposed appliance must natively support (without breakout) 8 x 1G Copper & 8 x 10G SFP+ Ports from day one. The 1G Copper ports should also support 10 SFP+ transceivers and the 10 SFP+ ports should also support 1 G Copper ports .The appliance should have 2 x 100G QSFP ports. Management,sync,HA etc ports should be additional. All the modules and transceivers should be provided from day one. (16x1 GCopper , 16x10G SFP , 2x100G QSFP in addition to the management , sync and HA ports	Requesting you to change the clause as "The 1G Copper ports should also support 10 SFP+ transceivers and the 10 SFP+ ports should also support 1 G Copper ports (Optional or at least for 50% ports)" Since interchanging the transceivers on all ports might not needed. (8x10Gb transceivers can accommodate 4x1GB copper)	Please refer to the revised technical specifications
38	7.2	The proposed firewall must define QoS traffic classes with: guaranteed bandwidth , maximum bandwidth , priority queuing & The proposed firewall must support real-time bandwidth statistics of QoS classes.	The proposed firewall must define QoS traffic classes with bandwidth rate limiting	Please refer to the revised technical specifications
39	1.8	The Firewall appliance should have certifications like ICSA / EAL4/CCNDPP	Optionally the Firewall appliance should have certifications like ICSA / EAL4/CCNDPP	Please be guided by the RFP
40	2.6	Firewall should support minimum of 2 and scale upto 4 security context or firewall should support creation of at least two firewall instances which shoul be scalable to 4.	Optionally the Firewall should support minimum of 2 and scale upto 4 security context or firewall should support creation of at least two firewall instances which shoul be scalable to 4.	Please refer to the revised technical specifications
41	8.2	Management solution should also have the following operational capabilities: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets	Management solution should also have the following operational capabilities: i. Rule-Reordering to improve the performance of the Firewall ii. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets	Clause Deleted

42	8.4	The solution has to provide for taking backups encrypted in SHA-256 format.	The solution has to provide for taking external backups in SHA-256 format.	Please refer to the revised technical specifications
43	Performance - 2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable.	**Query-1- Throughput consideration in terms of packet size and protocol should be similar for both Perimeter and Core firewall as same application traffic will pass through both tiers of firewall.** **Considering different benchmarks for sizing Perimeter and Core firewall may lead to variance in firewall performance at both tiers. Public document contains throughput based on enterprise mix of traffic and not HTTP 64K with all the features enabled. We can provide the undertaking on letterhead for the throughput.** **Query-2- Public document contains throughput based on enterprise mix of traffic and not HTTP 64K with all the features enabled. We can provide the undertaking on for the throughput.** Request to change the clause as "The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. **The performance must be based on HTTP traffic with a packet size of 64K. The claim has to be supported by publicly available documents published prior to the date of this RFP or OEM undertaking on Letterhead.** The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable."	Please refer to the revised technical specifications
44	Performance - 2.1	The proposed solution must provide minimum 30 Gbps of throughput (i.e. it should support 30 Gbps of ingress traffic and 30 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 1024 B. The claim has to be supported by publicly available documents published prior to the date of this RFP. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable.	The clause mentions throughput requirement of 30Gbps, with ingress throughput of 30Gbps and outgress throughput of 30Gbps simultaneously. The firewall is sized based on the total throughput of the appliance. Irrespective of the direction, traffic will hit and be processed by the CPU of the firewall. **Request you to confirm if the throughput should be considered at 60Gbps (aggregation of ingress + outgress traffic?**	Please refer to the revised technical specifications
45	High Availability - 3.13.5	The Firewall must support (redundant) Field replaceable (FRU) and hot swappable AC power supply and Hot swappable FAN. It must be supplied with both the Indian as well as European standard compatible power cords.	The proposed firewall will have in-built redundant FANs to ensure that the internal components are provided sufficient cooling and resiliency to failure. It does not give any additional benefit from a hardware standpoint. Request you to modify the clause as **" The Firewall must support (redundant) Field replaceable (FRU) and hot swappable AC power supply and redundant FAN. It must be supplied with both the Indian as well as European standard compatible power cords."**	Please be guided by the RFP
46	Threat Prevention - 6.4	The Proposed Solution should support over 40K IPS Signature.	**It is important for the solution to have effective security instead of relying on the number of IPS signatures. Similar criteria should be considered for Core firewall as considered for Perimeter firewall.** Request to rephrase the clause inline to the perimeter firewall specification as following **"Security effectiveness should be certified by NSS and should be more than 98.5%. In case NSS Lab reports are not published in the last two years prior to the date of this RFP, the OEM should have AAA rating published by Cyber rating report in 2021 /22 ."**	Please refer to the revised technical specifications
47	Threat Prevention 6.3	Shall support more than 4000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness	The current landscape is highly evolved and so is the number of applications. In the current generation of available technologies the number of applications support should atleast be 9000 or more to have better visibility. Requesting LIC team to amend the same.	Please be guided by the RFP
48	Threat Prevention 6.12	Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence	This point focuses more on endpoint needs. Requesting LIC team to remove it and keep it specific to Network Firewalls only.	Please refer to the revised technical specifications